CLAIMS

We claim:

1. A system for providing protected copying of material, comprising:

a preprocessing unit having an output and capable of providing copy-once functionality on a material before providing said material on said output; and

a recording unit coupled to said preprocessing unit output, and capable of searching for a copy-never indication in said material provided on said preprocessing unit output and copying said material unless said copy-never indication is found, but lacking capability to remark said material with a copy-no-more indication.

2. The system according to claim 1, wherein said copy-never indication comprises a copy-never watermark embedded in said material.

3. The system according to claim 1, wherein said copy-once functionality includes searching for a copy-once indication and a copy-no-more indication in said material, not providing said material on said preprocessing unit output if said copy-no-more indication is found, and remarking said material with said copy-no-more indication before providing said material on said preprocessing unit output if said copy-once indication is found and said copy-no-more indication is not found.

4. The system according to claim 3, wherein said copy-once indication comprises a copy-once watermark embedded in said material.

5. The system according to claim 3, wherein said copy-no-more indication comprises a copy-no-more watermark embedded in said material.

6. The system according to claim 3, wherein said preprocessing unit and said recording unit are further capable of establishing a secure channel between themselves to pass said material from said preprocessing unit to said recording unit if said preprocessing unit finds said copy-once indication and does not find said copy-no-more indication in said material.

7. The system according to claim 6, wherein said secure channel is established by performing an authentication and key exchange process between said preprocessing unit and said recording unit.

8. The system according to claim 7, wherein said authentication and key exchange process is a Diffie-Hellman process.

9. The system according to claim 1, wherein said recording unit is further capable of searching for a copy-once indication in said material, and copying said received material only if said copy-never indication and said copy-once indication are not found.

10. The system according to claim 9, wherein said recording unit is further capable of communicating information of finding said copy-once indication back to said preprocessing unit if a secure channel is established between said recording unit and said preprocessing unit.

11. The system according to claim 10, wherein said secure channel is established between said recording unit and said preprocessing unit before said copy-once indication is found in said material by said recording unit.

12. The system according to claim 10, wherein said secure channel is established between said recording unit and said preprocessing unit after said copy-once indication is found in said material by said recording unit.

13. The system according to claim 10, wherein said preprocessing unit is further capable of responding to said information of finding said copy-once indication received from said recording unit as though said preprocessing unit had itself found said copy-once indication.

14. The system according to claim 1, wherein said material comprises audio-visual content.

15. The system according to claim 1, wherein said preprocessing unit is included on an expansion board of a personal computer.

16. The system according to claim 15, wherein said expansion board is a video capture board.

17. The system according to claim 15, wherein said expansion board is a network board.

18. The system according to claim 1, wherein said preprocessing unit includes software running on a processor.

19. The system according to claim 1, wherein said preprocessing unit is included in a network appliance coupled to said recording unit.

20. The system according to claim 1, wherein said preprocessing unit is included in a set-top box coupled to said recording unit.

21. The system according to claim 1, wherein said recording unit is a DVD recordable drive.

22. A method implemented in a recording unit for providing protected copying of material, comprising:

detecting if a copy-never or copy-once indication is provided with a material;

if said copy-never indication is detected, then not allowing copying of said material;

if neither said copy-never nor said copy-once indication is detected, then allowing copying of said material; and

if said copy-once indication is detected, then transmitting information of said detection of said copy-once indication back to a sender of said material provided a secure channel is established with said sender, otherwise not allowing copying of said material.

23. The method according to claim 22, wherein said material comprises audio-visual content.

24. The method according to claim 22, wherein said copy-never indication comprises a copy-never watermark embedded in said material.

25. The method according to claim 22, wherein said copy-once indication comprises a copy-once watermark embedded in said material.

26. The method according to claim 22, wherein said recording unit is a DVD recordable drive.

27. The method according to claim 22, further comprising receiving said material from an expansion board included in a personal computer.

28. The method according to claim 27, wherein said expansion board is a video capture board coupled to said recording unit.

29. The method according to claim 27, wherein said expansion board is a network board coupled to said recording unit.

30. The method according to claim 22, further comprising receiving said material from a network appliance coupled to said recording unit.

31. The method according to claim 22, further comprising receiving said material from a set-top box coupled to said recording unit.

32. The method according to claim 22, wherein said transmitting information of said detection of said copy-once indication back to a sender of said material provided a secure channel is established with said sender, otherwise not allowing copying of said material, comprises:

if said copy-never indication is not detected and said copy-once indication is detected, then

if a secure channel is already established with said sender of said material, then transmitting information of said detection of said copy-once indication back to said sender of said material, and

if said secure channel is not already established with said sender of said material, then not allowing copying of said material.

33. The method according to claim 22, wherein said transmitting information of said detection of said copy-once

indication back to a sender of said material provided a secure channel is established with said sender, otherwise not allowing copying of said material, comprises:

if said copy-never indication is not detected and said copy-once indication is detected, then establishing a secure channel with said sender of said material;

if said secure channel cannot be established, then not allowing copying of said material; and

if said secure channel is established, then transmitting information of said detection of said copy-once indication back to said sender of said material.

34. The method according to claim 33, wherein said secure channel is established by performing an authentication and key exchange process between said sender of said material and said recording unit.

35. The method according to claim 34, wherein said authentication and key exchange process is a Diffie-Hellman process.

36. The method according to claim 22, further comprising:

detecting if a copy-no-more indication is provided with said material; and

if said copy-no-more indication is detected, then not allowing copying of said material.

37. The method according to claim 36, further comprising:

if said copy-never indication is not detected, said copy-once indication is detected, and said copy-no-more indication is not detected, then

if a secure channel is already established with said sender of said material, then transmitting information of said detection of said copy-once indication back to said sender of said material, and

if said secure channel is not already established with said sender of said material, then not allowing copying of said material.

38. The method according to claim 36, further comprising:

if said copy-never indication is not detected, said copy-once indication is detected, and said copy-no-more indication is not detected, then establishing a secure channel with a sender of said material;

if said secure channel cannot be established, then not allowing copying of said material; and

if said secure channel is established, then transmitting information of said detection of said copy-once indication back to said sender of said material.

39. The method according to claim 38, wherein said secure channel is established by performing an authentication and key exchange process between said sender of said material and said recording unit.

40. The method according to claim 39, wherein said authentication and key exchange process is a Diffie-Hellman process.

41. The method according to claim 37, wherein said copy-no-more indication comprises a copy-no-more watermark embedded in said material.

42. A recording unit for providing protected copying of material, comprising:

an input channel receiving a material for copying;

a primary detector coupled to said input channel to detect if a copy-never indication and a copy-once indication are provided with said material; and

compliance logic coupled to said primary detector and configured such that if said copy-never indication is detected, then preventing said material from being copied, and if neither said copy-never nor said copy-once indication is detected, then allowing said material to be copied.

43. The recording unit according to claim 42, wherein said material comprises audio-visual content.

44. The recording unit according to claim 42, wherein said copy-never indication comprises a copy-never watermark embedded in said material.

45. The recording unit according to claim 42, wherein said copy-once indication comprises a copy-once watermark embedded in said material.

46. The recording unit according to claim 42, wherein said recording unit is a DVD recordable drive.

47. The recording unit according to claim 42, wherein said material is received from an expansion board included in a personal computer.

48. The recording unit according to claim 47, wherein said expansion board is a video capture board coupled to said recording unit.

49. The recording unit according to claim 47, wherein said expansion board is a network board coupled to said recording unit.

50. The recording unit according to claim 42, wherein said material is received from a network appliance coupled to said recording unit.

51. The recording unit according to claim 42, wherein said material is received from a set-top box coupled to said recording unit.

52. The recording unit according to claim 42, further comprising secure channel logic configured such that:

if said copy-never indication is not detected and said copy-once indication is detected, then

if a secure channel has already been established with a sender of said material, then causing information of said detection of said copy-once indication to be transmitted back to said sender of said material, and

if a secure channel has not already been established with said sender of said material, then communicating with said compliance logic so as to not allow copying of said material.

53. The recording unit according to claim 42, further comprising secure channel logic configured such that:

if said copy-never indication is not detected and said copy-once indication is detected, then establishing a secure channel with a sender of said material;

if said secure channel cannot be established, then communicating with said compliance logic so as to not allow copying of said material;

if said secure channel is established, then causing information of said detection of said copy-once indication to be transmitted back to said sender of said material.

54. The recording unit according to claim 53, wherein said secure channel is established by performing an authentication and key exchange process between said sender of said material and said recording unit.

55. The recording unit according to claim 54, wherein said authentication and key exchange process is a Diffie-Hellman process.

56. The recording unit according to claim 42, further comprising a secondary detector coupled to said input channel to detect if a copy-no-more indication is provided with said material, and said compliance logic is further coupled to said secondary detector and configured such that if said copy-no-more indication is detected, then not allowing copying of said material.

57. The recording unit according to claim 56, wherein said compliance logic is further configured such that:

if said copy-never indication is not detected, said copy-once indication is detected, and said copy-no-more indication is not detected, then causing said secure channel logic to determine if a secure channel can be established with a sender of said material;

if said secure channel cannot be established, then not allowing copying of said material; and

if said secure channel can be established, then transmitting information of detection of said copy-once indication back to said sender of said material, and disabling said secure channel after such transmission.

58. The recording unit according to claim 57, wherein said secure channel is established by performing an authentication and key exchange process between said sender of said material and said recording unit.

59. The recording unit according to claim 58, wherein said authentication and key exchange process is a Diffie-Hellman process.

60. The recording unit according to claim 56, wherein said copy-no-more indication comprises a copy-no-more watermark embedded in said material.

61. The recording unit according to claim 42, wherein said compliance logic comprises a processor.

62. The recording unit according to claim 42, wherein said compliance logic comprises a state machine.

63. The recording unit according to claim 42, wherein said compliance logic comprises at least one logic circuit.

64. A system for providing protected copying of material, comprising:

a preprocessing unit having at least one input channel for receiving material and an output channel for providing an output, wherein said material is provided as said output if neither a copy-never indication nor a copy-once indication is detected as being provided with said material, said material is not provided as said output if either said copy-never indication is detected as being provided or said copy-once indication and a copy-no-more indication are both detected as being provided with said

material, and an encrypted version of said material including said copy-no-more indication is provided as said output and said output channel is configured to be a secure channel if said copy-once indication is detected and said copy-no-more indication is not detected prior to said inclusion with said material; and

a recording unit coupled to said output channel of said preprocessing unit and including a primary detector to detect if a copy-never indication and a copy-once indication are provided with said preprocessing unit's output; and compliance logic coupled to said primary detector and configured such that if said copy-never indication is detected, then not allowing said preprocessing unit's output to be copied, and if neither said copy-never nor said copy-once indication is detected, then allowing said preprocessing unit's output to be copied.

66. The system according to claim 64, wherein said compliance logic is further configured such that if said copy-once indication is detected, then establishing a secure channel with said preprocessing unit and passing information of said detection of said copy-once indication back to said preprocessing unit over said secure channel.

67. The system according to claim 66, wherein said preprocessing unit receives said information of said detection of said copy-once indication passed back by said recording unit, and provides said encrypted version of said material including said copy-no-more indication as said output over said secure channel.

68. The system according to claim 64, wherein said recording unit further includes a secondary detector to detect if a copy-no-more indication is provided with said preprocessing unit output, and said compliance logic is further configured such that if said copy-once indication is detected and said copy-no-more indication is not detected, then passing information of said detection of said copy-once indication back to said preprocessing unit over said secure channel if said secure channel has already been established.

69. The system according to claim 64, wherein said recording unit further includes a secondary detector to detect if a copy-no-more indication is provided with said preprocessing unit output, and said compliance logic is further configured such that if said copy-once indication is detected and said copy-no-more indication is not detected, then establishing a secure channel with said preprocessing unit and passing information of said detection of said copy-once indication back to said preprocessing unit over said secure channel.

70. The system according to claim 64, wherein said material comprises audio-visual content.

71. The system according to claim 64, wherein said copy-never indication comprises a copy-never watermark embedded in said material.

72. The system according to claim 64, wherein said copy-once indication comprises a copy-once watermark embedded in said material.

73. The system according to claim 64, wherein said copy-no-more indication comprises a copy-no-more watermark embedded in said material.

74. The system according to claim 64, wherein said preprocessing unit is an expansion board included in a personal computer.

75. The system according to claim 64, wherein said preprocessing unit is a network appliance coupled to said recording unit.

76. The system according to claim 64, wherein said preprocessing unit is a set-top box coupled to said recording unit.

77. The system according to claim 64, wherein said recording unit is a DVD recordable drive.

78. The system according to claim 64, wherein said secure channel is configured by performing an authentication and key exchange process between said preprocessing unit and said recording unit.

79. The system according to claim 64, wherein said compliance logic comprises a processor.

80. The system according to claim 64, wherein said compliance logic comprises a state machine.

81. The system according to claim 64, wherein said compliance logic comprises at least one circuit.